

CLAIMS:

1. A certification method, including:
receiving a public key of a public/private key pair generated by a system of a person;
5 processing said public key to generate a communicable code representative of said public
key;
identifying said person, said identifying including having said person convey said
communicable code; and
generating a digital certificate, said certificate including said public key.
- 10 2. A certification method as claimed in claim 1, wherein said identifying includes verifying
identification information of said person, and said certificate binds said identifying information
and said public key.
- 15 3. A certification method as claimed in claim 2, wherein said communicable code is a
limited character string.
4. A certification method as claimed in claim 3, wherein said communicable code is
generated using a secure one-way hash function.
- 20 5. A certification method as claimed in claim 1, including requesting generation of the
public/private key pair by the system of the person, in response to receiving a registration
request from the person.
- 25 6. A certification method as claimed in claim 5, wherein said registration request includes
said identifying information for said person.
7. A certification method as claimed in claim 1, wherein said identifying includes matching
a communicable code generated from said public key with the communicable code conveyed
30 by said person.
8. A certification method as claimed in claim 1, including sending said digital certificate
to said system of said person.

095725 002001

- 8 -

9. A certification method as claimed in claim 1, including sending said code to said system for said person.

10. A certification method as claimed in claim 9, wherein said sending includes transmitting
5 display data to said system for display of said communicable code by said system.

11. A certification method as claimed in claim 1, wherein said processing of said public key is executed by said system of said person.

10 12. A certification method as claimed in claim 1, wherein said conveying involves oral communication of said communicable code.

13. A certification method as claimed in claim 12, wherein the oral communication occurs during a telecommunications call.

15

14. A certification system, including:

means for receiving a public key of a public/private key pair generated by a system of a person;

means for processing said public key to generate a communicable code representative
20 of said public key; and

means for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

25 15. A certification system as claimed in claim 14, wherein said identifying includes verifying identification information of said person, and said certificate binds said identifying information and said public key.

16. A certification system as claimed in claim 15, wherein said communicable code is a
30 limited character string.

17. A certification system as claimed in claim 16, wherein said communicable code is generated using a secure one-way hash function.

09672510300100230152249360

- 9 -

18. A certification system as claimed in claim 14, including means for sending said code to said system for said person.

19. A certification system as claimed in claim 14, including means for requesting generation
5 of the public/private key pair by the system of the person, in response to receiving a registration request from the person.

20. A certification system as claimed in claim 19, wherein said registration request includes said identifying information for said person.

10

21. A certification system as claimed in claim 14, wherein said identifying includes matching a communicable code generated from said public key with the communicable code conveyed by said person.

15 22. A certification system as claimed in claim 14, including means for sending said digital certificate to said system of said person.

23. A certification system as claimed in claim 18, wherein said means for sending transmits display data to said system for display of said communicable code by said system.

20

24. A certification system as claimed in claim 14, wherein said conveying involves oral communication of said communicable code.

25. A certification system as claimed in claim 24, wherein the oral communication occurs
25 during a telecommunications call.

26. A certification system as claimed in claim 14, including means for executing said identifying.

30 27. A certification program stored on computer readable storage media, including:
code for receiving a public key of a public/private key pair generated by a system of a person;
code for processing said public key to generate a communicable code representative of

- 10 -

said public key; and

code for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

5

28. A certification program as claimed in claim 27, wherein said identifying includes verifying identification information of said person, and said certificate binds said identifying information and said public key.

10 29. A certification program as claimed in claim 28, wherein said communicable code is a limited character string.

30. A certification program as claimed in claim 29, wherein said communicable code is generated using a secure one-way hash function.

15

31. A certification program as claimed in claim 27, including code for sending said code to said system for said person.

32. A certification program as claimed in claim 27, including code for requesting generation
20 of the public/private key pair by the system of the person, in response to receiving a registration request from the person.

33. A certification program as claimed in claim 32, wherein said registration request includes said identifying information for said person.

25

34. A certification program as claimed in claim 27, wherein said identifying includes matching a communicable code generated from said public key with the communicable code conveyed by said person.

30 35. A certification program as claimed in claim 27, including code for sending said digital certificate to said system of said person.

36. A certification program as claimed in claim 31, wherein said code for sending transmits

0985725-082001

display data to said system for display of said communicable code by said system.

37. A certification program as claimed in claim 27, wherein said conveying involves oral communication of said communicable code.

5

38. A certification program as claimed in claim 37, wherein the oral communication occurs during a telecommunications call.

39. A certification program as claimed in claim 27, including code for executing said
10 identifying.

40. An identification process, including:
receiving a public key of a public/private key pair and identifying information of a
person;

15 deriving a communicable code from said public key; and
having said person convey said communicable code.

41. An identification process as claimed in claim 40, including comparing a communicable
code derived from the public key with the conveyed communicable code, and issuing a digital
20 certificate binding the public key and identifying information when the codes match.

42. An identification process as claimed in claim 41, wherein said communicable code is
a limited character string.

25 43. An identification process as claimed in claim 42, wherein said communicable code is
generated using a secure one-way hash function.

44. An identification process, including:
generating a communicable code from a public key of a public/private key pair; and
30 binding said public key to identifying information of a person when said person conveys
said communicable code.

0985722.082001
T00230" 52225869